REMARKS/ARGUMENTS

In the Office action dated November 10, 2004, Claims 1 - 3, 14, 16 - 22, 27, 29 and 30 were rejected under 35 U.S.C. § 102. Claims 4 - 6, 9 - 12 and 24 were rejected under 35 U.S.C. § 103. Claims 7, 8, 13, 15, 23, 26, 28 and 31 were deemed allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

By this Amendment, Applicants have amended the specification and Claim 1. Reconsideration and reexamination are hereby requested for Claims 1 - 31 that are pending in this application.

Amendments

Applicants have amended the Specification to correct several typographical errors and other language. Applicants submit that no new matter has been added as the amended language is clearly supported by the original context of the Specification. Applicants have amended Claim 1 to correct a typographical error.

35 U.S.C. §102 Rejections of Claims 1 - 3, 16 - 22 and 27

The Examiner has rejected Claims 1 - 3, 16 - 22, and 27 under 35 U.S.C. §102(e) as being anticipated by Silverbrook et al., U.S. Patent No. 6,334,190 (hereafter "Silverbrook"). Claims 1, 16 and 27 are independent claims.

Claim 1 recites:

1. An authentication engine architecture for a

multi-loop, multi-round authentication algorithm, comprising:

a first instantiation of a multi-round authentication algorithm hash round logic in an inner hash engine;

a second instantiation of a multi-round authentication algorithm hash round logic in an outer hash engine;

a dual-frame payload data input buffer configured for loading one new data block while another data block is being processed in the inner hash engine;

an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations; and

a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines.

The first and second elements of Claim 1 recite two separate instantiations of a multi-round authentication algorithm hash round logic: one in an inner hash engine and one in an outer hash engine. The Examiner contends that these elements are disclosed in col. 7, lines 3 - 5 and col. 11, lines 9 - 27 of Silverbrook. Applicants respectfully disagree.

The cited passages of Silverbrook state that the output of one round is input to the next round (the first passage) and lists the standard HMAC algorithm (the second passage). These passages do not, however, state or suggest that separate inner and outer hash engines are used. Indeed, the terminology of inner and outer hash engines does appear anywhere in

Silverbrook. Accordingly, these elements of Claim 1 are not taught or suggested by Silverbrook.

The third element of Claim 1 was found by the Examiner to be disclosed in col. 7, lines 3 - 5 and col. 45, lines 2 - 6 of Silverbrook. Applicants respectfully differ on this point. Col.7, lines 3-5 state: "In many cases, X is broken into blocks of a particular size, and compressed over a number of rounds, with the output of one round being the input to the next." Col. 45, lines 2-6 state: "Since we only deal with 2 types of messages, our padding can be constant 0s. In addition, the optimized version of the SHA-1 algorithm is used, where only 16 32-bit words are used for temporary storage. These 16 registers are loaded directly by the optimized HMAC-SHA1 hardware."

The first passage does not mention when loading occurs and the second passage talks of simultaneous loading but does not mention "a dual-frame payload data input buffer configured for loading one new data block while another data block is being processed in the inner hash engine ...." As such, this element of Claim 1 is not taught or suggested by Silverbrook.

The fourth element of Claim 1 was found by the Examiner in col. 45, lines 2 - 6 of Silverbrook stating: "Since we only deal with 2 types of messages, our padding can be constant 0s. In addition, the optimized version of the SHA-1 algorithm is used, where only 16 32-bit words are used for temporary storage. These 16 registers are loaded directly by the optimized HMAC-SHA1 hardware." This passage discusses the number and size of the words and the fact that they are directly loaded and stored in temporary storage. It does not disclose "an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations". Thus, this element of Claim 1 is not taught or suggested by Silverbrook.

The fifth element of Claim 1 has been rejected as disclosed by col. 38, lines 8 - 13 of Silverbrook stating: "If a given System only produces about n R-values, the sparse lookup ROM required is 10n bytes multiplied by the number of different values for M. The time taken to build the ROM depends on the amount of time enforced between calls to RD." This passage has no mention of "a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines." The ROM of Silverbrook is for use with a "sparse lookup table." Col. 37, line 43. Also, "The attacker will therefore need to find a valid Authentication Chip and call it for each of the values in R." Col. 37, lines 63-65. As best understood this teaches consecutive lookups. In the lines cited, Col 38, lines 8-13, Silverbrook is discussing the total number of lookups and the time they take but not how the lookups are conducted.

In view of the above, the Applicants submit that Claim 1 is not anticipated by or obvious in view of Silverbrook. Claims 2 and 3 that depend on Claim 1 also are patentable over Silverbrook for the reasons set forth above. In addition, these dependent claims are patentable over Silverbrook for the additional limitations that these claims contain.

The Examiner also concluded that independent Claim 16 was anticipated by Silverbrook.

As discussed above, at least, the element "processing the fixed-size data blocks using a multi-loop, multi-round authentication engine architecture having a hash engine core comprising an inner hash engine and an outer hash engine" has not been taught by the cited passages of Silverbrook.

The last element of Claim 16 has been rejected as disclosed by col. 11, lines 9 - 27 of Silverbrook presenting the standard HMAC algorithm. This algorithm presents a series of steps taken in succession and does not teach a "multi-round logic to schedule addition computations to be conducted in parallel with round operations."

In view of the above, the Applicants submit that Claim 16 is not anticipated by or obvious in view of Silverbrook. Claims 17 - 22 that depend on Claim 16 also are patentable over Silverbrook for the reasons set forth above. In addition, these dependent claims are patentable over Silverbrook for the additional limitations that these claims contain.

The Examiner also concluded that independent Claim 27 was anticipated by Silverbrook at col. 11, lines 9-27. As argued for Claim 16, the passage cited does not disclose a "hash round logic for a multi-round authentication algorithm configured to schedule addition computations to be conducted in parallel with round operations." In view of the above, the Applicants submit that Claim 27 is not anticipated by or obvious in view of Silverbrook.

35 U.S.C. §102 Rejections of Claims 14, 29 and 30

Claims 14, 29, and 30 have been rejected under 35 U.S.C. §102(b) as being anticipated by Schneier at pages 442-445. Claims 14 and 29 are independent claims.

Claim 14 is an independent product claim. Schneier, on page 444, discloses a figure depicting one conventional SHA operation. The text states: "Figure 18.7 shows one operation. Shifting the variables accomplishes the same thing as MD5 does by using different variables in different locations. After all of this, a, b, c, d, and e are added to A, B, C, D, and E respectively, and the algorithm continues with the next block of data. The final output is the concatenation of A, B, C, D, and E." There is no further explanation of the figure or the process in Schneier.

In contrast Claim 14 is directed to an improved SHA1 architecture. For example, Claim 14 recites, in part: "in successive SHA1 rounds, registers having the critical path are alternative." Schneier does not disclose what happens to the data in a subsequent round or in successive rounds. Moreover, Schneier does not teach or suggest the alternative processing that Applicants have invented. In view of the above, the Applicants submit that Claim 14 is not anticipated by or obvious in view of Schneier.

Claim 29 is an independent method claim that has been rejected for the same reasons as Claim 14 because the Examiner finds it substantially equivalent to Claim 14.

Schneier, on pages 442-445, has no mention of timing. The relevant disclosure of Schneier on the cited pages is limited to Figure 18.7 and the passage already quoted. Independent method

Claim 29 is distinguished from Schneier, at least, by "providing data paths from said five state registers such that four of the five data paths from the registers in any SHA1 round are not timing critical."

In view of the above, the Applicants submit that Claim 29 is not anticipated by or obvious in view of Schneier. Claim 30 that depends on Claim 29 also is patentable over Schneier for the reasons set forth above. In addition, Claim 30 is patentable over Schneier for the additional limitations that Claim 30 contains. For example, Schneier does not disclose that "in successive SHA1 rounds, registers having the critical path are alternative."

35 U.S.C. §103 Rejections:

The Examiner has rejected Claims 4 and 5 and 9 - 12 under 35 U.S.C. §103 as being unpatentable over Silverbrook in view of Sait et al., a scientific article (hereafter “Sait”). Claims 6 and 24 have been rejected under 35 U.S.C. §103 as being patentable over Silverbrook in view of Schneier.

Claims 4 and 5

The Applicants submit that the invention as claimed in Claim 4 is neither taught, described nor suggested by Silverbrook in view of Sait.

Claim 4 calls for "The authentication engine architecture of Claim 1, wherein at least one of the inner and outer hash engines is configured to implement hash round logic including at least one addition module comprising: a plurality of carry save adders for computation of partial products; and a carry look-ahead adder for computation and propagation of a final sum." Applicants respectfully submit that Silverbrook does not suggest Claim 1 from which Claim 4 depends for the reasons cited in the above discussion pertaining to Claim 1.

Moreover, the passages of Silverbrook that, according to the Examiner, disclose Claim 1 do not suggest mechanisms for expediting the operations. Nor does the HMAC algorithm shown in Silverbrook (col. 11 lines 9-27) mention adding or multiplying operations. The operations of HMAC are padding, XOR, and hash operations. The Hash functions, starting on col. 8 line 53, are not described at the detailed operations level and as they mention no operations, hardly do they motivate a reader to look for ways of expediting those unmentioned operations. Generally speaking and subject to exceptions, Silverbrook is focused on maximizing security and does not address speed. Silverbrook claims to "operate within a specific clock speed range" (Abstract) to prevent certain types of attacks (col. 1 lines 49-60) and not to speed up the hash process.

Sait is directed to a new technique for high speed 2's complement multiplication. It becomes more useful as the size of the multiplier increases; for a multiplier of size n, the number of multiplications is n/3 and the number of additions required for the multiplication is reduced from n to 2n/3. Figure 3 of Sait shows parallel multiplications in the "pp cells" that precalculate partial products. Claim 4 is distinguished, at the least, by reciting "including at least one addition module ... for computation and propagation of a final sum." There is no suggestion in these references or the art that the multiplication techniques taught in Sait should or could be used in an addition module as claimed in Claim 4.

In short, Silverbrook and Sait do not disclose or suggest Claim 4 and there is no suggestion in either reference or in the art or any motivation to combine these references. Even if the two were combined, their combination would not disclose or suggest Claim 4.

Accordingly, the Applicants submit that Claim 4 is not unpatentable over Silverbrook in view of Sait. Claim 5 that depends on Claim 4 also is patentable over the cited references for the reasons set forth above. In addition, Claim 5 is patentable over the cited references for the additional limitations that Claim 5 contains. For example, the cited reference considered independently or in combination do not teach or suggest "addition computations are conducted in parallel with round operations."

Claims 6 and 24

The Applicants submit that the invention as claimed in Claim 6 is neither taught, described nor suggested by Silverbrook in view of Schneier.

Claim 6 depends from Claim 3 which in turn depends from Claim 1. As explained above, Silverbrook does not foray into the details of hash algorithms and consequently does not teach or suggest Claim 1. Further, as also explained above, Schneier discloses and discusses only one round of hash operations and says nothing about what could happen in successive rounds.

Schneier, therefore, does not teach or suggest the additional limitations of Claim 6.

In short, Silverbrook and Schneier do not disclose or suggest Claim 6 either independently or in combination. Accordingly, the Applicants submit that Claim 6 is not unpatentable over Silverbrook in view of Schneier.

The Applicants submit that the invention as claimed in Claim 24 is neither taught, described nor suggested in Silverbrook in view of Schneier.

Claim 24 depends from Claim 22 which in turn depends from Claim 16. Claim 16 is not disclosed or suggested by Silverbrook or Schneier, considered either independently or in combination. For example, neither Silverbrook nor Schneier in the pages pointed out by the Examiner covers any of the internal workings of a hash algorithm. For example, neither reference suggests the "implement multi-round logic to schedule addition computations to be conducted in parallel with round operations" of Claim 16. Moreover, as discussed above, the cited references teach nothing regarding "four of the five data paths from the registers in any SHA1 round are not timing critical" as claimed in Claim 24. Accordingly, the Applicants submit that Claim 24 is not unpatentable over Silverbrook in view of Schneier.

Claims 9-12

Claim 9 in an independent claim. Claims 10 - 12 depend on Claim 9. The Applicants submit that the invention as claimed in Claim 9 is neither taught, described nor suggested by Silverbrook in view of Sait.

Silverbrook and Sait, considered either independently or in combination, do not disclose or suggest Claim 9. Silverbrook does not go into the detail of a hash algorithm and Sait, while not mentioning authentication at all, is about faster multiplications not additions. As explained above, there is no suggestion in either reference or in the art or any motivation to combine these references. Even if the two were combined, their combination would not disclose or suggest Claim 9. For example, the cited references to not disclose or suggest that an addition module may comprise "a plurality of carry save adders for computation of partial products, and a carry look-ahead adder for computation and propagation of a final sum" as claimed in Claim 9.

Accordingly, the Applicants submit that Claim 9 is not unpatentable over Silverbrook in view of Sait. Claims 10 - 12 that depend on Claim 9 also are patentable over the cited references for the reasons set forth above. In addition, these claims are patentable over the cited references for the additional limitations that these claims contain.

Not every element of the above claims that is thought to be novel and can be distinguished from the references is discussed either because no reference was cited against them or in the interest of brevity.

CONCLUSION

In view of the above it is submitted that the claims are patentably distinct over the cited references and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By ____________________
Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/cah
FS PAS605842.1-*-02/3/05 9:03 AM